IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

Sakari POUSSA et al.	Group Art Unit: Unassigned
Application No.: New Application	Examiner: Unassigned
Filed: November 25, 2003	Attorney Dkt. No.: 60279-00069

For: REMOTE IPSEC SECURITY ASSOCIATION MANAGEMENT

CLAIM FOR PRIORITY UNDER 35 USC § 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450   November 25, 2003

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified patent application and the priority provided in 35 U.S.C. §119 is hereby claimed:
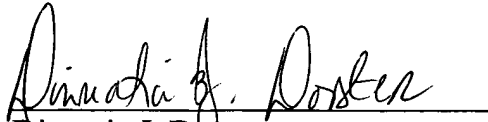
Patent Application No. 20031361 filed on September 22, 2003 **in Finland**

In support of this claim, a certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 U.S.C. §119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Please charge any fee deficiency or credit any overpayment with respect to this paper to Counsel's Deposit Account No. 50-2222.

Respectfully submitted,

Dinnatia J. Doster
Registration No. 45,263

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DJD:cct

Enclosure: Priority Document (1)

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 30.9.2003

E T U O I K E U S T O D I S T U S
P R I O R I T Y   D O C U M E N T

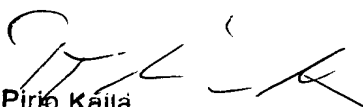|	
Hakija Applicant	**Nokia Corporation** **Helsinki**
Patenttihakemus nro Patent application no	20031361
Tekemispäivä Filing date	22.09.2003
Kansainvälinen luokka International class	**H04L**
Keksinnön nimitys Title of invention	

"Remote IPSec security association management"
(IPSec-turva-assosiaatioiden kaukohallinta)

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä
Patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä,
patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the
description, claims, abstract and drawings originally filed with the
Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

Maksu   50 €
Fee   50 EUR

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001
Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry
No. 1027/2001 concerning the chargeable services of the National Board of Patents and
Registration of Finland.

L 3

TITLE OF THE INVENTION:

REMOTE IPSEC SECURITY ASSOCIATION MANAGEMENT

BACKGROUND OF THE INVENTION:

5   Field of the Invention:

The invention relates to communications tech-
nology. In particular, the invention relates to a
novel and improved method and system for remotely and
transparently managing security associations of Inter-
10   net Protocol Security.

Description of the Related Art:

Internet Protocol Security, also referred to
15   as IPSec or IPsec, is a framework for providing secu-
rity in IP networks at network layer. IPSec is devel-
oped by The Internet Engineering Task Force (IETF).
RFC documents (Request for Comments, RFC) 2401 to 2409
by IETF describe IPSec.
20   IPSec provides confidentiality services and
authentication services to IP traffic. These services
are provided by protocols called Authentication Header
(AH, described in RFC 2402), which essentially allows
authentication of the sender of data, and Encapsulat-
25   ing Security Payload (ESP, described in RFC 2406),
which supports both authentication of the sender and
encryption of data.
Authentication Header and Encapsulating Secu-
rity Payload require session keys in order to operate.
30   The session keys are typically generated via key man-
agement protocols, such as Internet Key Exchange (IKE,
described in RFC 2409). A key management protocol
called Authentication and Key Agreement (AKA) may also
be used, particularly in communication networks based
35   on 3GPP (3rd Generation Partnership Project) systems.

Additionally, there are other key management protocols that may be used.

In addition to the protocols mentioned above, IPSec uses security associations to provide its serv-

5 ices. An IPSec security association comprises such information as traffic selectors, cryptographic transforms, session keys and session key lifetimes. A key management application is responsible for negotiating the creation and deletion of an IPSec security asso-

10 ciation.

Typically IPSec services and key management protocols may be found e.g. in dedicated security gateways, servers, desktop computers and handheld terminals. In prior art, whatever the target device, the

15 IPSec services and key management protocols are tied together in the sense that they are co-located in the same device. So it also follows that the communication mechanism between IPSec services and an associated key management protocol is local.

20 In a distributed computing environment, however, network element functionality benefits from an architecture in which various applications are located in dedicated devices. For example, applications requiring cryptographic operations are typically located

25 in a special purpose device containing suitable hardware and software for the task. Other applications may require more CPU processing power and may therefore be located in a different type of special purpose device. Further, in a distributed computing environment, ap-

30 plications typically require services from each other in order to provide the network element functionality.

In the case of network layer security, IPSec and its associated key management protocols are examples of applications requiring services from each

35 other. It would be beneficial to arrange IPSec service on a device capable of high-speed symmetric cryptography, and to arrange its associated key management pro-

tocol in another device with high CPU power and/or
asymmetric cryptography acceleration. Yet, as men-
tioned above, in prior art IPSec service and the key
management protocol used by it are located in the same

5 computing device. There are many key management proto-
cols, each with different characteristics. If, as is
the case with prior art, all these various key manage-
ment protocols have to be located in the same device
as the IPSec service, network element design, imple-

10 mentation and deployment become inefficient and some-
times even impossible.

Thus there is an obvious need for a more so-
phisticated approach allowing IPSec service and its
associated key management protocols to be arranged on

15 different devices, particularly in distributed comput-
ing environments. Further, it would be beneficial to
be able to transparently do this distribution of IPSec
and its associated key management.

20 **SUMMARY OF THE INVENTION:**

The present invention concerns a method and a
system for remotely and transparently managing secu-
rity associations of Internet Protocol Security.

The system comprises one or more application

25 devices. Each application device comprises at least
one management client for issuing security association
management requests.

The system further comprises a service de-
vice. The service device comprises an Internet Proto-

30 col Security service means for providing one or more
Internet Protocol Security services. The service de-
vice further comprises a management server for receiv-
ing the issued requests and for responding, in connec-
tion with the Internet Protocol Security service

35 means, to the received requests.

The system further comprises a communication network for connecting the application devices to the service device.

In an embodiment of the invention at least
5 one application device further comprises an interface means for providing an interface via which the at least one management client associated with the application device and the management server communicate with each other. Thus, the interface means according
10 to the present invention and the management server according to the present invention allow such distribution of IPSec and its associated key management that is transparent to the management client and to the Internet Protocol Security service means. In other
15 words, present management clients do not need to be modified for them to be able use services provided by the Internet Protocol Security service means even though said Internet Protocol Security service means may be located on another device than said management
20 client.

In an embodiment of the invention the security association management requests include requests for adding security associations, requests for deleting security associations, and/or requests for query-
25 ing about security associations.

In an embodiment of the invention the interface means includes data structures used in communication between the management client and the management server, and the interface means are implemented as a
30 software library linked dynamically or statistically into a corresponding management client.

In an embodiment of the invention the interface means are arranged to use sockets for communication with the management server.

35 In an embodiment of the invention the Internet Protocol Security service means and the management

server are arranged to use a local communication chan-
nel for communication with each other.

In an embodiment of the invention at least
one application device comprises two or more manage-
ment clients, at least two of which management clients
utilize session key management protocols different
from each other.

In an embodiment of the invention said commu-
nication network is a Local Area Network.

The invention makes it possible to remotely
manage IPSec security associations. IPSec and its as-
sociated key management can be transparently distrib-
uted to separate computing devices. Thus each comput-
ing device can be optimized to run a specific applica-
tion. This in turn increases performance and flexibil-
ity.

Yet, the invention does not preclude utiliz-
ing standard prior art solutions when beneficial. E.g.
in smaller configurations the IPSec and its associated
key management may still be co-located in the same de-
vice. This may be accomplished by switching a remote
communication channel to a local one. The switch is
transparent to the applications, thus minimizing de-
velopment effort, and increasing flexibility.

BRIEF DESCRIPTION OF THE DRAWINGS:

The accompanying drawings, which are included
to provide a further understanding of the invention
and constitute a part of this specification, illus-
trate embodiments of the invention and together with
the description help to explain the principles of the
invention. In the drawings:

Fig 1 is a block diagram illustrating a sys-
tem according to one embodiment of the invention, and

Fig 2 illustrates a method according to one
embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS:

Reference will now be made in detail to the embodiments of the invention, examples of which are illustrated in the accompanying drawings.

5   Figure 1 illustrates a system for remotely and transparently managing security associations of Internet Protocol Security according to an embodiment of the invention. In the exemplary embodiment of the invention illustrated in Figure 1 the system comprises 10 two application devices APP_DEV_1 and APP_DEV_2. The application device APP_DEV_1 comprises one management client MNG_CL_1 for issuing security association management requests, whereas the application device APP_DEV_2 comprises two management clients MNG_CL_2 15 and MNG_CL_3. The security association management requests issued by management clients MNG_CL_1, MNG_CL_2 and MNG_CL_3 include requests for adding security associations, requests for deleting security associations, and/or requests for querying about security associations. In the exemplary embodiment of the invention illustrated in Figure 1 the management clients MNG_CL_1, MNG_CL_2, MNG_CL_3 each utilize a different session key management protocol.

Internet Protocol Security is typically utilized for example by IP Multimedia Subsystem (IMS) of a 3GPP system based telecommunication network. In such a case, a user equipment (not illustrated) may communicate with the application device APP_DEV_1 or APP_DEV_2 by using a key management protocol, and the 30 end result of this communication is then forwarded to the service device SRV_DEV by the application device APP_DEV_1 or APP_DEV_2. Thus, in this case, the application device APP_DEV_1 or APP_DEV_2 may be running a server portion of the key management protocol, whereas 35 the user equipment may be running a client portion of the key management protocol. The user equipment may

use its own local mechanism to communicate the end result to its own IPSec service.

In the exemplary embodiment of the invention illustrated in Figure 1 the system further comprises a
5   service device SRV_DEV. The service device SRV_DEV comprises an Internet Protocol Security service means IPSEC for providing one or more Internet Protocol Security services. The service device SRV_DEV further comprises a management server MNG_SRV for receiving
10   the issued requests and for responding, in connection with the Internet Protocol Security service means IPSEC, to the received requests. The system further comprises a communication network CN for connecting the application devices to the service device.
15   In the exemplary embodiment of the invention illustrated in Figure 1 the application devices APP_DEV_1 and APP_DEV_2 each further comprise an interface means IF for providing an interface via which the management clients MNG_CL_1, MNG_CL_2, MNG_CL_3
20   and the management server MNG_SRV communicate with each other. Further in the exemplary embodiment of the invention illustrated in Figure 1 the interface means IF include data structures (not illustrated) used in communication between the management clients MNG_CL_1,
25   MNG_CL_2, MNG_CL_3 and the management server MNG_SRV, and the interface means IF are each implemented as a software library (not illustrated) which may be linked either dynamically or statistically into a management client.
30   Further in the exemplary embodiment of the invention illustrated in Figure 1 the interface means IF are each arranged to use sockets for communication with the management server MNG_SRV, and the Internet Protocol Security service means IPSEC and the manage-
35   ment server MNG_SRV are arranged to use a local communication channel for communication with each other.

Further, as illustrated in Figure 1, external
IP traffic EXT entering the system is preferably
routed via the service device SRV_DEV.

Figure 2 illustrates a method for remotely
5 and transparently managing security associations of
Internet Protocol Security according to an embodiment
of the invention.

One or more Internet Protocol Security serv-
ices are provided in a service device, phase 20. Secu-
10 rity association management requests are issued from
one or more application devices, phase 21. The appli-
cation devices have been securely connected to the
service device by a communication network.

The issued requests are received in the serv-
15 ice device, phase 22. The received requests are re-
sponded to in the service device in connection with
the provided Internet Protocol Security services,
phase 23.

In the exemplary embodiment of the invention
20 illustrated in Figure 2 the security association man-
agement requests issued from an application device,
and/or corresponding responses are communicated via an
interface associated with said application device.

It is obvious to a person skilled in the art
25 that with the advancement of technology, the basic
idea of the invention may be implemented in various
ways. The invention and its embodiments are thus not
limited to the examples described above, instead they
may vary within the scope of the claims.

L 4

WHAT IS CLAIMED IS:

1. A system for remotely and transparently managing security associations of Internet Protocol Security, wherein the system comprises:

5   one or more application devices, each comprising at least one management client for issuing security association management requests,

a service device comprising an Internet Protocol Security service means for providing one or more

10   Internet Protocol Security services, and a management server for receiving said issued requests and for responding, in connection with said Internet Protocol Security service means, to said received requests, and

a communication network for connecting said

15   application devices to said service device.

2. The system according to claim 1, wherein at least one application device further comprises an interface means for providing an interface via which said at least one management client associated with

20   said application device and said management server communicate with each other.

3. The system according to claim 1, wherein said security association management requests include requests for adding security associations, requests

25   for deleting security associations, and/or requests for querying about security associations.

4. The system according to claim 2, wherein said interface means are arranged to use sockets for communication with said management server.

30   5. The system according to claim 2, wherein said interface means includes data structures used in communication between said management client and said management server.

6. The system according to claim 2, wherein

35   said interface means are implemented as a software library linked dynamically or statistically into a corresponding management client.

7. The system according to claim 1, wherein said Internet Protocol Security service means and said management server are arranged to use a local communication channel for communication with each other.

5   8. The system according to claim 1, wherein at least one application device comprises two or more management clients, at least two of which management clients use session key management protocols different from each other.

10   9. The system according to claim 1, wherein said communication network is a Local Area Network.

         10. A method for remotely and transparently managing security associations of Internet Protocol Security, wherein the method comprises the steps of:

15   providing one or more Internet Protocol Security services in a service device,

         issuing security association management requests from one or more application devices, said one or more application devices being connected to said

20   service device by a communication network,

         receiving said issued requests in said service device, and

         responding, in connection with said provided Internet Protocol Security services, to said received

25   requests in said service device.

         11. The method according to claim 10, wherein security association management requests issued from an application device, and/or corresponding responses are communicated via an interface associated with said

30   application device.

         12. The method according to claim 10, wherein said security association management requests include requests for adding security associations, requests for deleting security associations, and/or requests

35   for querying about security associations.

L5

/

ABSTRACT OF THE DISCLOSURE

The present invention concerns
a method and a system for remotely and
transparently managing security associa-
tions of Internet Protocol Security. The

5   system comprises one or more application
devices, each of which comprises at
least one management client for issuing
security association management re-
quests. The system further comprises a

10   service device comprising an Internet
Protocol Security service means for pro-
viding one or more Internet Protocol Se-
curity services, and a management server
for receiving the issued requests and

15   for responding, in connection with the
Internet Protocol Security service
means, to the received requests. The
system further comprises a communication
network for securely connecting the ap-
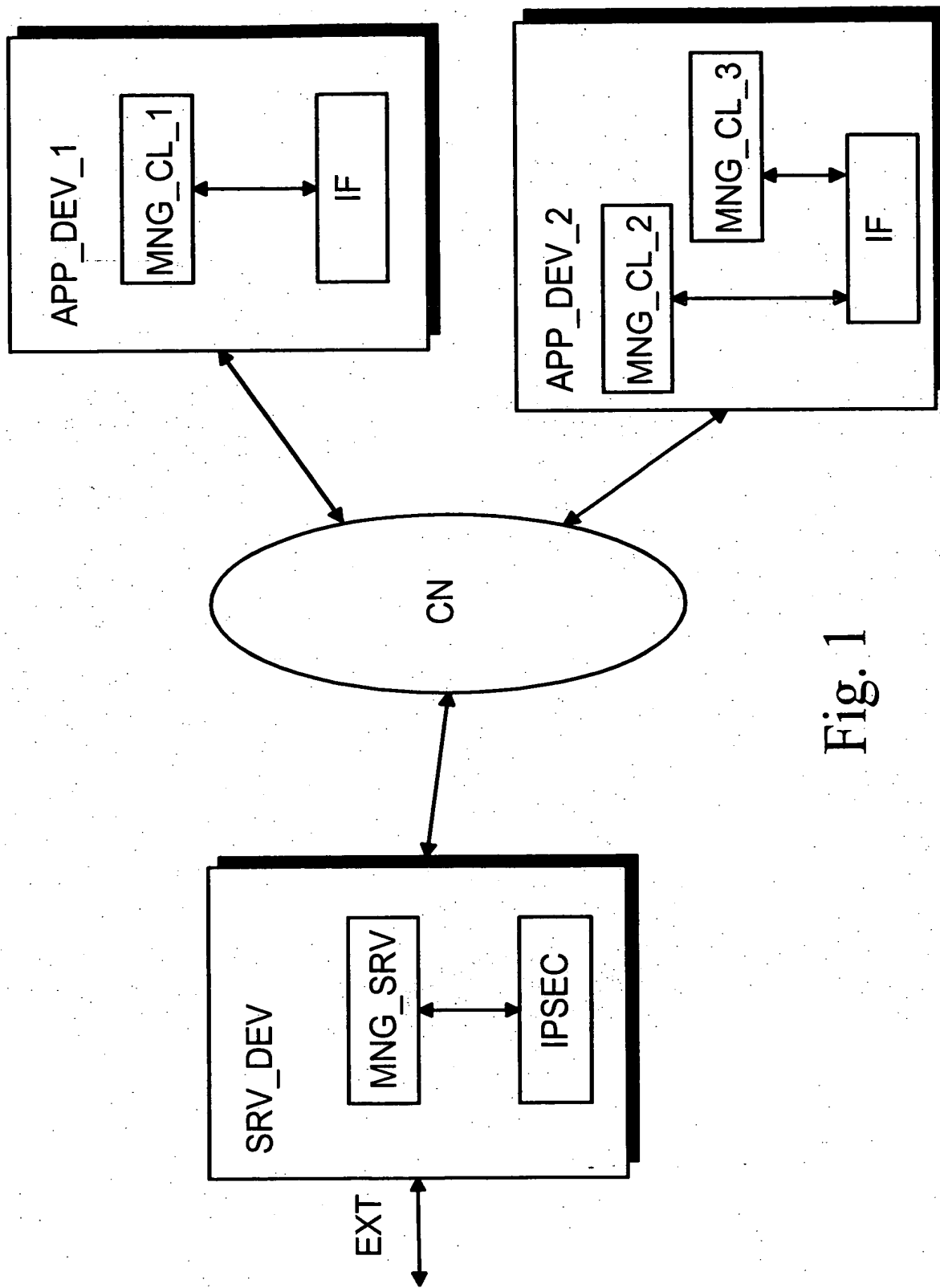
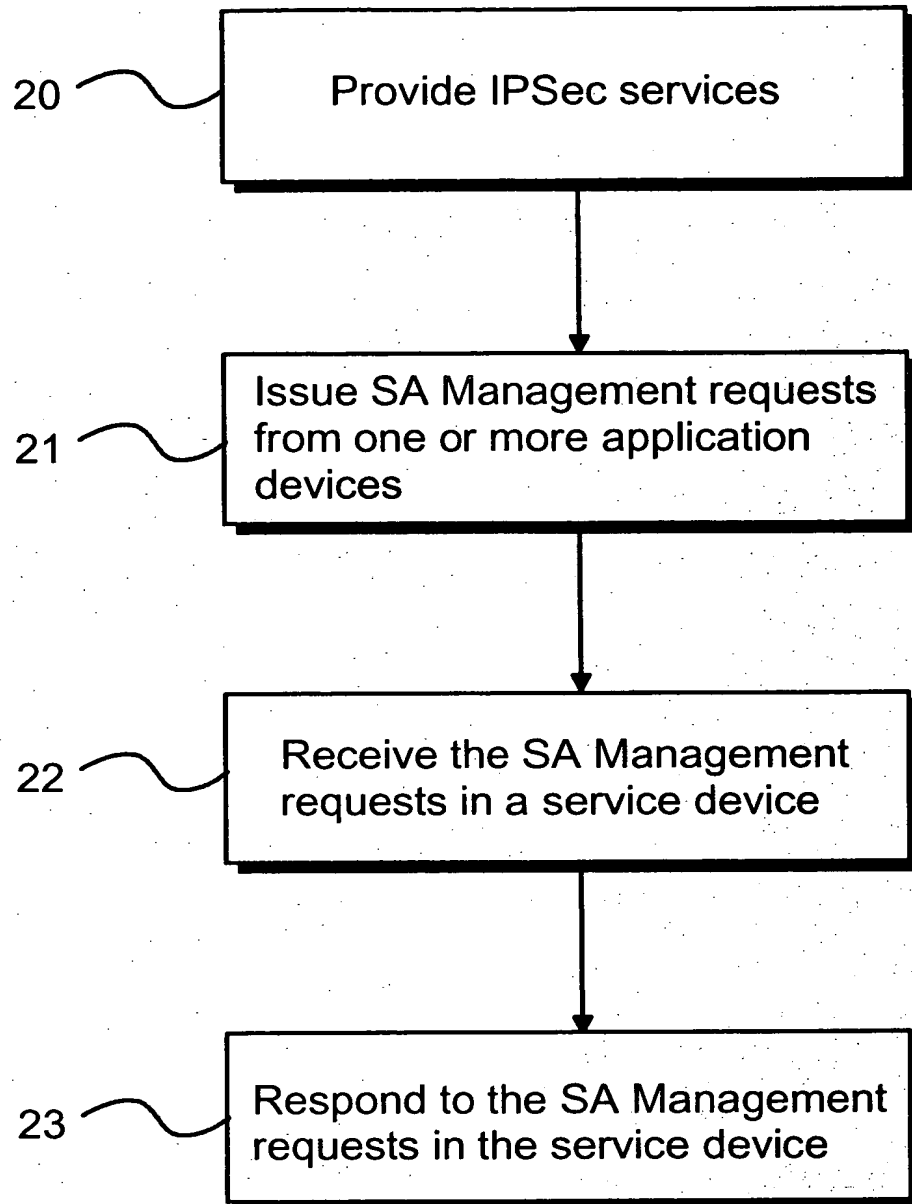20   plication devices to the service device.

Fig. 1

```
┌─────────────────────────────────┐
20 ──  │      Provide IPSec services      │
       └─────────────────────────────────┘
                      │
                      ▼
       ┌─────────────────────────────────┐
21 ──  │ Issue SA Management requests     │
       │ from one or more application     │
       │ devices                          │
       └─────────────────────────────────┘
                      │
                      ▼
       ┌─────────────────────────────────┐
22 ──  │ Receive the SA Management        │
       │ requests in a service device     │
       └─────────────────────────────────┘
                      │
                      ▼
       ┌─────────────────────────────────┐
23 ──  │ Respond to the SA Management     │
       │ requests in the service device   │
       └─────────────────────────────────┘
```

Fig. 2